Hon. John C. Coughenour

Presented to the Court by the foreman of the Grand Jury in open Court, in the presence of the Grand Jury and FILED in the U.S. DISTRICT COURT at Seattle, Washington.

MAY 19 20 11
WILLIAM M. McCOOL, Clerk
By _______ Deputy

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. DMITRY OLEGOVICH ZUBAKHA, aka Eraflame, aka Dima-k17, aka DDService, and SERGEY VIKTOROVICH LOGASHOV, aka Jjoker, Defendants.	NO. CR10-0078JCC SUPERSEDING INDICTMENT

The Grand Jury charges that:

COUNT 1

(Conspiracy to Intentionally Cause Damage Without Authorization to a Protected Computer)

A. The Offense

1. Beginning at a time uncertain, but beginning no later than June 6, 2008, and continuing until on or about August 15, 2008, within the Western District of Washington and elsewhere, DMITRY OLEGOVICH ZUBAKHA, aka Eraflame, aka Dima-k17, aka DDService, and SERGEY VIKTOROVICH LOGASHOV, aka Jjoker, did knowingly and willfully conspire, combine, confederate, and agree together with others, known and unknown to the Grand Jury, to commit offenses against the United States, to wit: intentionally causing damage to a protected computer, in violation of

Title 18, United States Code, Sections 1030(a)(5)(A)(i), 1030(b), and 1030(c)(4)(A), and committed acts in furtherance of that conspiracy.

B. Background

At all times material herein,

1. Amazon.com is a world leader in the online retailing of consumer products. Amazon.com operates retail websites, including www.amazon.com, and offers programs that enable third parties to sell products on its websites. Amazon.com earns revenues in a number of ways, including through retail sales of goods through its websites and by charging fees to sellers who list goods for sale on the Amazon.com websites. Amazon.com is headquartered in Seattle, WA. Amazon.com's business model relies upon online commerce, and the success of that model depends upon the ability of its customers to access its websites and conduct transactions on those websites quickly, reliably, and securely. The content on Amazon.com's websites is provided and supported by a network of server computers, ("webservers"), which computers are used in interstate and foreign commerce and communication.

2. EBay is a major online commercial and auction business, which describes itself as "the worlds' largest online marketplace." Headquartered in San Jose, CA, eBay serves 90 million online users, worldwide, who access the eBay website to post items for sale or auction, or who access the eBay website to purchase the items posted there for sale or auction. Ebay earns revenues by charging a small fee for the transactions that take place through their website. EBay's business model relies upon online commerce, and the success of that model depends upon the ability of its customers to access its website and conduct transactions on that website quickly, reliably, and securely. The content on cBay's website is provided and supported by a network of server computers, (webservers), which computers are used in interstate and foreign commerce and communication.

3. Priceline.com is a major online travel-related business, headquartered in Norwalk, CN. Through its website, Priceline.com provides consumers with the ability to purchase airline tickets or cruise or vacation packages, or make hotel or car reservations. Priceline.com earns revenues by keeping a small percentage of the cost, or charging a small

handling fee, for transactions that take place through their website. Priceline.com's business model relies upon online commerce, and the success of that model depends upon the ability of its customers to access its website and conduct transactions on that website quickly, reliably, and securely. The content on Priceline.com's website is provided and supported by a network of server computers, (webservers), which computers are used in interstate and foreign commerce and communication.

4. DMITRY OLEGOVICH ZUBAKHA is an individual residing in Moscow, Russia.

5. SERGEY VIKTOROVICH LOGASHOV is an individual residing in Moscow, Russia.

Internet Websites and the Webservers that Host Them

6. Websites contain information (data) that is available to computer users via the Internet and the world wide web. The information (data) that appears to a user who accesses a website is stored on a specialized type of computer, called a webserver. When a request to view a website, or a webpage within that site, is received by a webserver, the webserver compiles and transmits the appropriate data, in a user friendly form, back to the computer (and user) who made that particular request.

7. The demand placed on a webserver to respond to a request can vary, according to the type of data or service requested. A response to a request for a webpage that contains only text, for example, can be transmitted relatively easily and quickly. If a request is made for a webpage with a large number of graphic images, however, the webserver must compile, process and transmit much more data. The requisite data components may, in fact, be stored on many different webservers. As a result, requests for these webpages place a much greater burden on, and usurp a larger share of a webserver's capacity.

8. Companies with high volume traffic websites often require a large number of webservers to fully and reliably respond to requests made by visitors to view graphic webpages, and to conduct interactive transactions through their websites. These webservers may be located

in multiple geographic locations, but are networked to provide cohesive support to the company website and reliably provide the level of services normally requested through it.

Internet Protocol Addresses and Proxy Servers

9. Computers that are connected to the Internet need to be able to "find" one another in order to communicate. **"Internet Protocol addresses" ("IP addresses")** serve this function. Every computer connected to the Internet is assigned a unique 32-bit IP address, that consists of four sets of from one to three digits separated by a period. Data that accompanies an Internet communication will typically include the destination, as well as the originating IP address. The originating IP address can in turn be used to identify the source of the particular communication.

10. A **proxy server** is a computer or server computer that acts as a proxy (intermediary) in the transmission of Internet communications. Proxy servers can therefore be used to conceal the true originating IP address - and therefore the source - of a communication made over the Internet. For example, an individual who wants to conceal his originating IP address can route his communication to and through a proxy server - or even through a succession of proxy servers - on route to the final destination. Data identifying the originating IP address of the communication will be replaced with data that instead identifies the IP address of the proxy server/s through which the communication was routed. As a result, it may then be impossible to identify the true source of that Internet communication.

Other Terminology Relating to Computer Attacks and Attackers

11. **Bot Computer**. A "bot" ("robot') computer is a computer that has been infected with some kind of (typically malicious) software or code and is thereafter subject to control by someone other than the true owner. The true owner of the computer may not even be aware of the bot infection, because he may remain able to use the computer as he did before it was infected, (although speed or performance may be compromised). At the same time, however, the bot controller may also be using the infected bot computer for malicious purposes - to commit Distributed Denial of Service ("DDoS") attacks, send spam e-mail, or function as a proxy server, without the true computer owner's knowledge or consent.

12. **Botnet**. A "botnet" is a network of bot computers. The computers are harnessed and can be used en masse, in a coordinated fashion, to deliver Internet-based attacks, including DDoS attacks, to transmit spam, or as networks of proxy servers.

13. **Distributed Denial of Service ("DDoS") Attack.** DDoS attacks are malicious attacks against websites, made in ways that are intended to overwhelm the capacities of a webserver to process legitimate Internet traffic. As a result, visitors and would-be customers of the website and its sponsoring business are "denied service" - and are consequently unable to place orders for merchandise or conduct other types of transactions through the affected website during the pendency of the attack. For companies who conduct a large volume of business online, the financial impact of a DDoS attack can be severe.

14. Malicious computer attackers ("hackers") have developed a variety of DDoS attack methods, of varying levels of severity and sophistication. Many of these methodologies involve botnets. One or more botnets can be used, for example, to send extraordinary volumes of traffic to website servers, so that all of the available webserver capacity is consumed simply in receiving the traffic. Another method of attack is to use botnets to transmit an extraordinary volume of requests for information from the webservers, so that the servers become overwhelmed in processing the responses to those data requests. Whatever the methodology, services to legitimate website visitors and would-be customers can be impaired or even completely denied by such an attack, until such time as the victim entity can defeat the attack and restore its webservers and systems to normal operations. This may take minutes, hours, or sometimes even days.

15. Hackers launch DDoS attacks for a variety of reasons. In some cases, they wage DDoS attacks against prominent online commercial targets simply to build and promote their reputations as hackers, with a goal of then "renting" botnets or marketing their DDoS expertise and hacking services to others. Hackers sometimes launch DDoS attacks against other hackers, or hacker groups, for like reasons - to promote their reputations - or, as part of a feud, or to seek revenge against other hackers or hacker groups. Hackers also commonly DDoS online commercial companies to extort them, based on the premise that it will be "cheaper" for a

company to meet an extortion demand than to suffer the losses both to sales and to reputation that could result from a "successful" and lengthy DDoS attack. In such cases, the victim company typically will receive a communication - by e-mail or by telephone - after an attack has begun, with an offer for "technical" or "IT assistance" in solving the DDoS problem that the company is experiencing.

16. **Hacking Forums.** Hacker forums are websites, typically accessible only to members, that are devoted to topics related to hacking. Hackers can visit these sites and communicate with others sharing these mutual interests. The hacking forums typically include various "pages" where members of the forum can post and answer questions on botnets, DDoS attacks, and other hacking-related issues. Hackers can also post advertisements for hacking services, along with the prices for the same.

17. **Online Nicknames ("Nics").** Hackers typically are identified in their communications by their online "nic" (nickname or screen name). A hacker's reputation (or "street cred") within the hacking community and on hacking forums is linked to his nic. The history of that nic can help hackers communicate and build trust with each other. Consequently, a hacker's "nic" is currency that is highly valued and zealously protected. Some hackers will use multiple nics or alias names in order to engage in conduct or make statements within the hacking community that they want to appear as coming from others. For example, a hacker may use one nic, within a hacking forum, to praise the malicious services that he is advertising for sale, under another of his nics.

C. Object and Purpose of the Conspiracy

18. The object of the conspiracy was to launch DDoS attacks against major online retail companies, by using botnets to transmit particular types of commands to the webservers of those companies, in artificially high volumes, with the intention of impairing or destroying the ability of those webservers to provide data and normal online retail services to the companies' customers. DMITRY OLEGOVICH ZUBAKHA, aka Eraflame, aka Dima-k17, aka DDService, and SERGEY VIKTOROVICH LOGASHOV, aka Jjoker, intended by these DDoS attacks to build

and enhance their reputation as hackers; to extort, or attempt to extort money from the online companies they victimized; and/or to gain financially in other ways, such as through the sale of their hacking services.

D. Manner and Means of the Conspiracy

19. It was part of the conspiracy that DMITRY OLEGOVICH ZUBAKHA, aka Eraflame, aka Dima-k17, aka DDService, and SERGEY VIKTOROVICH LOGASHOV, aka Jjoker, conspired and agreed to launch DDoS attacks against the websites of prominent online retail companies, including Amazon.com, eBay, and Priceline.com, beginning no later than June 6, 2008, and continuing through July 21, 2008.

20. It was further part of the conspiracy that DMITRY OLEGOVICH ZUBAKHA, aka Eraflame, aka Dima-k17, aka DDService, and SERGEY VIKTOROVICH LOGASHOV, aka Jjoker, made preliminary visits to, and reconnoitered the websites that they targeted for DDoS attacks, and when doing so, utilized proxy servers to conceal their true originating IP addresses, and thus the true origin of those communications.

21. It was further part of the conspiracy that DMITRY OLEGOVICH ZUBAKHA, aka Eraflame, aka Dima-k17, aka DDService, and SERGEY VIKTOROVICH LOGASHOV, aka Jjoker, themselves created, and/or otherwise gained access to botnets, in order to launch the agreed-upon DDoS attacks against their targeted online victim companies.

22. It was further part of the conspiracy that DMITRY OLEGOVICH ZUBAKHA, aka Eraflame, aka Dima-k17, aka DDService, and SERGEY VIKTOROVICH LOGASHOV, aka Jjoker, issued commands to the bots they used for their DDoS attacks, to make requests, through the websites and webservers of their targeted online victim companies, to display webpages that contained particularly large numbers of graphic or picture files, because requests of that type would place extraordinary burdens on the targeted webservers. DMITRY OLEGOVICH ZUBAKHA, aka Eraflame, aka Dima-k17, aka DDService, and SERGEY VIKTOROVICH LOGASHOV, aka Jjoker, knew and intended that the massive burdens they thus placed on the targeted webservers would consequently impair the ability of those computers to provide data to,

and support commercial transactions by and with would-be online customers of the targeted companies.

23. It was further part of the conspiracy that DMITRY OLEGOVICH ZUBAKHA, aka Eraflame, aka Dima-k17, aka DDService, and SERGEY VIKTOROVICH LOGASHOV, aka Jjoker, did launch DDoS attacks of the type described above against Amazon.com on or about June 6, and again on June 9, 2008; against eBay on or about June 6, 2008; and against Priceline.com on or about July 21, 2008.

24. It was further part of the conspiracy that DMITRY OLEGOVICH ZUBAKHA, aka Eraflame, aka Dima-k17, aka DDService, periodically visited and made communications to and in online hacker forums, during the period from at least June 6, 2008, to and until August 15, 2008, in which he acknowledged and confirmed his involvement in hacking activities, posted credit card numbers obtained from hacking attacks, offered malicious botnets for rent, and otherwise promoted himself and his expertise as an accomplished hacker for the purpose of marketing his malicous hacking services.

25. It was further part of the conspiracy that after initiating the DDoS attack on Priceline.com, on July 21, 2008, DMITRY OLEGOVICH ZUBAKHA, aka Eraflame, aka Dima-k17, aka DDService, and SERGEY VIKTOROVICH LOGASHOV, aka Jjoker, placed a telephone call to Priceline.com; stated that the phone call was from "Sergey"; and stated further that “Sergey” was an "information technology consultant" who was willing to “assist them” with their "network problems."

E. Overt Acts

26. In furtherance of the conspiracy and to achieve the objects thereof, at least one of the coconspirators committed or caused to be committed, in the Western District of Washington, and elsewhere, at least one of the following overt acts, among others:

27. On or about June 6, 2008, at about 10:23 a.m. (PST), DMITRY OLEGOVICH ZUBAKHA, aka Eraflame, aka Dima-k17, aka DDService, and

SERGEY VIKTOROVICH LOGASHOV, aka Jjoker, launched a DDoS attack against the website and webservers of Amazon.com, that continued until Amazon.com was able to successfully mitigate the attack at around 2:55 p.m. (PST) on June 6, 2008. During the attack, the bots involved in the attack requested large and resource intensive webpages on a magnitude of 600% to 1000% of normal traffic levels. As a result, Amazon.com webservers were overwhelmed, and legitimate customers were unable to access the website and complete their e-commerce transactions during the pendency of the attack. Amazon.com suffered financial losses exceeding $5,000.00 as a result.

28. On or about June 9, 2008, at about 10:06 a.m. (PST), DMITRY OLEGOVICH ZUBAKHA, aka Eraflame, aka Dima-k17, aka DDService, and

SERGEY VIKTOROVICH LOGASHOV, aka Jjoker, launched a DDoS attack against the website and webservers of Amazon.com, that continued at some level until Amazon.com was able to finally and fully mitigate the attack on June 12, 2008. During the attack, the bots involved in the attack requested large and resource intensive webpages, overwhelming Amazon.com webservers. Orders from Amazon.com customers dropped significantly, as legitimate customers were unable to access the website and complete their e-commerce transactions during the pendency of the attack. Amazon.com suffered financial losses exceeding $5,000.00 as a result.

29. On or about June 10, 2008, DMITRY OLEGOVICH ZUBAKHA, aka Eraflame, aka Dima-k17, aka DDService, under the nic, "Eraflame," acknowledged and confirmed in communications made in a hacker forum that he was behind the DDoS attacks on Amazon.com.

All in violation of Title 18, United States Code, Section 371.

COUNT 2

(Intentionally Causing and Attempting to Cause Damage to a Protected Computer and Thereby Causing Loss in Excess of $5,000)

On or about June 6, 2008, within the Western District of Washington and elsewhere, DMITRY OLEGOVICH ZUBAKHA, aka Eraflame, aka Dima-k17, aka DDService, and

SERGEY VIKTOROVICH LOGASHOV, aka Jjoker, knowingly caused and attempted to cause the transmission of a program, information, code, and command, and as a result of that conduct, intentionally caused and attempted to cause damage, without authorization, to webserver computers belonging to, and used in interstate commerce and communications by Amazon.com, and by such conduct caused an aggregate loss to Amazon.com of at least $5,000 in value during a one-year period.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i), 1030(b), 1030(c)(4)(A), and 2.

COUNT 3

(Intentionally Causing and Attempting to Cause Damage to a Protected Computer and Thereby Causing Loss in Excess of $5,000)

On or about June 9, 2008, within the Western District of Washington and elsewhere, DMITRY OLEGOVICH ZUBAKHA, aka Eraflame, aka Dima-k17, aka DDService, and SERGEY VIKTOROVICH LOGASHOV, aka Jjoker, knowingly caused and attempted to cause the transmission of a program, information, code, and command, and as a result of that conduct, intentionally caused and attempted to cause damage, without authorization, to webserver computers belonging to, and used in interstate commerce and communications by Amazon.com, and by such conduct caused an aggregate loss to Amazon.com of at least $5,000 in value during a one-year period.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i), 1030(b), 1030(c)(4)(A), and 2.

COUNT 4

(Possession of Fifteen or More Unauthorized Access Devices)

On or about October 12, 2009, within the Western District of Washington and elsewhere, DMITRY OLEGOVICH ZUBAKHA, aka Eraflame, aka Dima-k17, aka DDService, knowingly and with intent to defraud, possessed and attempted to possess fifteen or more unauthorized access devices, and by such conduct affected interstate and foreign commerce, in that, on that date, DMITRY OLEGOVICH ZUBAKHA, aka Eraflame, aka Dima-k17, aka DDService, possessed credit card track data for over 28,000 credit cards, which included credit card account numbers for accounts that were established through and issued by the Boeing Employees Credit Union, in the Western District of Washington, and which credit card account numbers were used to make fraudulent purchases in locations outside the State of Washington, and outside the United States.

All in violation of Title 18, United States Code, Sections 1029(a)(3), 1029(b)(1), and 1029(c)(1)(A)(i).

/ /

/ /

/ /

/ /

/ /

/ /

/ /

/ /

/ /

/ /

/ /

/ /

/ /

/ /

/ /

/ /

/ /

COUNT 5

(Aggravated Identity Theft)

On or about October 12, 2009, within the Western District of Washington and elsewhere, DMITRY OLEGOVICH ZUBAKHA, aka Eraflame, aka Dima-k17, aka DDService, knowingly transferred, possessed and used, without lawful authority, a means of identification of another person, to wit, the personally identifiable credit card number ****-****-****-9668, belonging to K.A. of Lake Stevens, WA, within the Western District of Washington, during and in relation to a felony listed in Title 18, United States Code, Section 1028A(c), to wit, Access Device Fraud, in violation of Title 18, United States Code, Section 1029.

All in violation of Title 18, United States Code, Section 1028A(a)(1).

A TRUE BILL:

DATED: May 19, 2011

Signature of the Foreperson redacted pursuant
to the policy of the Judicial Conference

FOREPERSON

JENNY A. DURKAN
United States Attorney

CARL BLACKSTONE
Assistant United States Attorney

KATHRYN A. WARMA
Assistant United States Attorney